(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2001－282619
（P2001－282619A）
(43)公開日　平成13年10月12日(2001.10.12)

(51)Int.Cl.[7]	識別記号	ＦＩ		テーマコード（参考）
Ｇ０６Ｆ　12/14	３１０	Ｇ０６Ｆ　12/14	３１０Ｚ	５Ｂ０１７
15/00	３３０	15/00	３３０Ａ	５Ｂ０８５
Ｇ０９Ｃ　1/00	６４０	Ｇ０９Ｃ　1/00	６４０Ｄ	５Ｊ１０４
				９Ａ００１

審査請求　未請求　請求項の数５　ＯＬ　（全 12 頁）

(21)出願番号　特願2000－94313(P2000－94313)

(22)出願日　平成12年３月30日(2000.3.30)

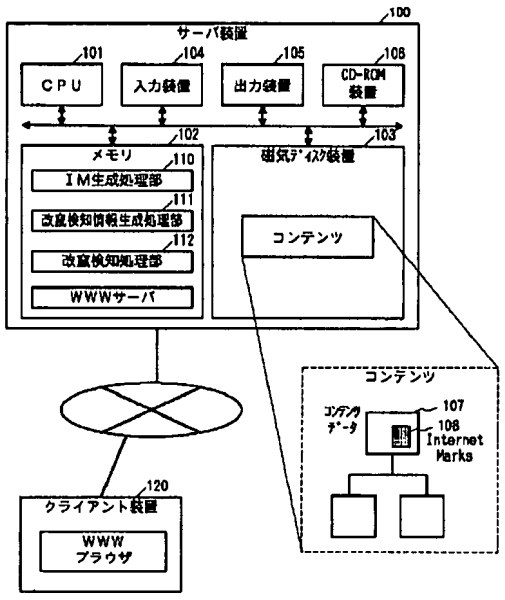
(71)出願人　000005108
株式会社日立製作所
東京都千代田区神田駿河台四丁目６番地
(72)発明者　篠田　隆志
東京都江東区新砂一丁目６番27号　株式会社日立製作所公共システム事業部内
(72)発明者　豊島　久
東京都江東区新砂一丁目６番27号　株式会社日立製作所公共システム事業部内
(74)代理人　100083552
弁理士　秋田　収喜

最終頁に続く

(54)【発明の名称】　コンテンツ改竄検知方法及びその実施装置並びにその処理プログラムを記録した記録媒体

(57)【要約】
【課題】　コンテンツの改竄を早期発見することが可能な技術を提供する。
【解決手段】　コンテンツの改竄を検知するコンテンツ改竄検知方法において、複数のコンテンツの現在の構成または内容に対応する改竄検知情報を生成するステップと、当該コンテンツの登録または更新時の構成または内容に対応する改竄検知情報と前記生成した改竄検知情報とを比較して当該コンテンツの改竄を検知するステップとを有するものである。

図１



1

【特許請求の範囲】

【請求項１】　コンテンツの改竄を検知するコンテンツ改竄検知方法において、

複数のコンテンツの現在の構成または内容に対応する改竄検知情報を生成するステップと、当該コンテンツの登録または更新時の構成または内容に対応する改竄検知情報と前記生成した改竄検知情報とを比較して当該コンテンツの改竄を検知するステップとを有することを特徴とするコンテンツ改竄検知方法。

【請求項２】　コンテンツの改竄を検知するコンテンツ改竄検知方法において、

あるコンテンツについて、その改竄を検知する為の改竄検知情報が生成済みであるかどうかを検査するステップと、当該コンテンツの改竄検知情報の有無を検査するステップとを有することを特徴とするコンテンツ改竄検知方法。

【請求項３】　コンテンツの改竄を検知するコンテンツ改竄検知方法において、

コンテンツの現在の内容に対応する改竄検知情報を生成するステップと、当該コンテンツの登録または更新時の内容に対応する改竄検知情報と前記生成した改竄検知情報とを比較して当該コンテンツの改竄を検知した場合に、当該コンテンツの要求元、登録元または更新元に通知するステップとを有することを特徴とするコンテンツ改竄検知方法。

【請求項４】　コンテンツの改竄を検知するコンテンツ改竄検知装置において、

複数のコンテンツの現在の構成または内容に対応する改竄検知情報を生成する改竄検知情報生成処理部と、当該コンテンツの登録または更新時の構成または内容に対応する改竄検知情報と前記生成した改竄検知情報とを比較して当該コンテンツの改竄を検知する改竄検知処理部とを備えることを特徴とするコンテンツ改竄検知装置。

【請求項５】　コンテンツの改竄を検知するコンテンツ改竄検知装置としてコンピュータを機能させる為のプログラムを記録したコンピュータ読み取り可能な記録媒体において、

複数のコンテンツの現在の構成または内容に対応する改竄検知情報を生成する改竄検知情報生成処理部と、当該コンテンツの登録または更新時の構成または内容に対応する改竄検知情報と前記生成した改竄検知情報とを比較して当該コンテンツの改竄を検知する改竄検知処理部としてコンピュータを機能させる為のプログラムを記録したことを特徴とする記録媒体。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明はコンテンツの改竄を検知するコンテンツ改竄検知装置に関し、特にインターネットのホームページで表示されるコンテンツに対して行われた改竄を検知するコンテンツ改竄検知装置に適用して有効な技術に関するものである。

2

【０００２】

【従来の技術】従来、個人を始め官公庁や多くの企業等がWWW(World Wide Web)サーバ装置にホームページを開設し、各種の情報発信を行っている。官公庁や企業が開設するホームページで公開される内容は、簡単なお知らせから公式な発表と同等な内容のものまで多岐に渡っており、インターネットにアクセスすることにより誰でもこれらの情報を得ることができる様になっている。

【０００３】これらの官公庁や企業が開設するホームページの内容は、その官公庁や企業が外部に対して正式に発信しているものと考えられる為、その内容に誤りがあったり、外部の人間によるサーバへの不正侵入によりホームページの内容が改竄された場合、著しい信用の低下を招く場合がある。この為、簡単な広報活動の為にホームページを開設している場合であっても、そのセキュリティ対策を十分にとっておく必要があるが、近年では外部の人間が官公庁等のサーバに不正侵入し、ホームページの内容を改竄するという事件が相次いでいる。

【０００４】なお厳密な電子データの真正性の認証を可能とすると共に、その真正性を視覚的に電子データの利用者に表現する認証可能な電子データの生成方法については、特開２０００－７８１２５号公報に記載されている。その概要は、Webページや商標などの電子マークＢを認証するための認証情報にデジタル署名を付加したものを、電子マークＡに不可視の電子透かしとして埋め込んだ後、真正性を視覚的に表現する電子マークＡを、電子マークＢに可視の電子透かしとして埋め込むものである。

【０００５】

【発明が解決しようとする課題】前記の様なホームページの内容を改竄される事件での大きな問題は、ホームページを公開するサーバのセキュリティ対策が甘いということに加え、公開しているホームページの量が膨大である為、一部のホームページが改竄されてもそれに気付くのが遅れがちになるという点にある。

【０００６】本発明の目的は上記問題を解決し、コンテンツの改竄を早期発見することが可能な技術を提供することにある。

【０００７】本発明の他の目的は改竄検知情報の除去による改竄の隠蔽を防止することが可能な技術を提供することにある。

【０００８】本発明の他の目的は改竄が行われた位置を特定することが可能な技術を提供することにある。

【０００９】

【課題を解決するための手段】本発明は、コンテンツの改竄を検知するコンテンツ改竄検知装置において、複数のコンテンツの構成または内容の改竄を検知するものである。

【００１０】本発明では、複数のコンテンツの登録また

は更新時にそれらの構成または内容に対応する改竄検知情報を生成しておく。そして、所定の時刻になる等の所定の条件が成立した場合に、前記生成した改竄検知情報を参照し、当該コンテンツの現在の構成または内容に対応する改竄検知情報を生成した後、前記参照した改竄検知情報と前記生成した改竄検知情報とを比較して当該コンテンツの改竄を検知し、当該コンテンツの改竄を通知する。

【００１１】例えば、公開しているホームページで表示される複数のコンテンツの登録または更新時に、それらのファイル構造や各ファイルの内容のハッシュ値を改竄検知情報として生成してＩＭ(Internet-Marks)に埋め込み、ホームページのトップページにそのＩＭを貼付しておく。

【００１２】そして、常駐プログラム等の処理により所定の時刻になる等の所定の条件が成立した場合に、前記貼付したＩＭ中の登録または更新時のファイル構造や各ファイルの内容のハッシュ値を参照し、また現在のファイル構成や各ファイルの内容のハッシュ計算を行う。次に、前記参照したＩＭ中の登録または更新時のファイル構造や各ファイルの内容のハッシュ値と、前記生成した現在のファイル構造や各ファイルの内容のハッシュ値とを比較し、もし前記生成した現在のハッシュ値がＩＭに埋め込まれているハッシュ値と異なる場合は、システム管理者に通報すると共に、トップページのＩＭのデザインを変更してコンテンツの改竄が行われたことを閲覧者に知らせる。

【００１３】前記の様に本発明では、システム管理者等の人間が常時チェックしなくても、公開しているホームページの一部が改竄された場合に、改竄が行われたことを即座に通知することが可能となり、不正の早期発見ができる。また同時に、閲覧者に対してもホームページの改竄が行われたことを即座に知らせることが可能となる。

【００１４】以上の様に本発明のコンテンツ改竄検知装置によれば、複数のコンテンツの構成または内容の改竄を検知するので、コンテンツの改竄を早期発見することが可能である。

【００１５】

【発明の実施の形態】（実施形態１）以下に複数のコンテンツの改竄を検知する実施形態１のコンテンツ改竄検知装置について説明する。

【００１６】図１は本実施形態のコンテンツ改竄検知装置の概略構成を示す図である。図１に示す様に本実施形態のサーバ装置１００は、ＣＰＵ１０１と、メモリ１０２と、磁気ディスク装置１０３と、入力装置１０４と、出力装置１０５と、ＣＤ－ＲＯＭ装置１０６と、コンテンツデータ１０７と、ＩＭ１０８とを有している。

【００１７】ＣＰＵ１０１は、サーバ装置１００全体の動作を制御する装置である。メモリ１０２は、サーバ装置１００全体の動作を制御する際にその為の各種処理プログラムやデータをロードする記憶装置である。磁気ディスク装置１０３は、前記各種処理プログラムやデータを格納しておく記憶装置である。

【００１８】入力装置１０４は、複数のコンテンツの改竄を検知する為の各種入力を行う装置である。出力装置１０５は、複数のコンテンツの改竄の検知に伴う各種出力を行う装置である。ＣＤ－ＲＯＭ装置１０６は、前記各種処理プログラムを記録したＣＤ－ＲＯＭの内容を読み出す装置である。

【００１９】コンテンツデータ１０７は、クライアント装置１２０からの要求に応じて公開されるページの内容を示すデータである。ＩＭ１０８は、複数のコンテンツデータ１０７に対応する改竄検知情報を埋め込んだ画像データである。

【００２０】またサーバ装置１００は、ＩＭ生成処理部１１０と、改竄検知情報生成処理部１１１と、改竄検知処理部１１２とを有している。

【００２１】ＩＭ生成処理部１１０は、複数のコンテンツの登録または更新時の構成または内容に対応する改竄検知情報を埋め込んだＩＭを生成する処理部である。改竄検知情報生成処理部１１１は、複数のコンテンツの構成または内容に対応する改竄検知情報を生成する処理部である。

【００２２】改竄検知処理部１１２は、複数のコンテンツの登録または更新時の構成または内容に対応する改竄検知情報と、当該コンテンツの現在の構成または内容に対応する改竄検知情報とを比較して当該コンテンツの改竄を検知する処理部である。

【００２３】サーバ装置１００をＩＭ生成処理部１１０、改竄検知情報生成処理部１１１及び改竄検知処理部１１２として機能させる為のプログラムは、ＣＤ－ＲＯＭ等の記録媒体に記録され磁気ディスク等に格納された後、メモリにロードされて実行されるものとする。なお前記プログラムを記録する記録媒体はＣＤ－ＲＯＭ以外の他の記録媒体でも良い。

【００２４】コンテンツデータを管理・公開するサーバ装置１００と、コンテンツデータを閲覧するクライアント装置１２０は、インターネット等のネットワークにより相互にデータの送受信が可能であるものとする。

【００２５】サーバ装置１００には、クライアント装置１２０からの要求に応じてコンテンツデータの公開を行うＷＷＷサーバが実装され、クライアント装置１２０には、サーバ装置からコンテンツデータを受信し、表示するＷＷＷブラウザが実装される。

【００２６】また、サーバ装置１００に接続される磁気ディスク装置１０３には、複数のコンテンツデータ１０７を格納し、そのうちの１つ、例えばコンテンツのトップページに、複数のコンテンツデータ１０７に対応する改竄検知情報を埋め込んだインターネットマークである

ＩＭ１０８を貼付することとする。

【００２７】図２は本実施形態のＩＭ生成処理部１１０の処理手順を示すフローチャートである。図２に示す様にサーバ装置１００のＩＭ生成処理部１１０は、複数のコンテンツの登録または更新時の構成または内容に対応する改竄検知情報を埋め込んだＩＭを生成する処理を行う。

【００２８】ステップ２０１でＩＭ生成処理部１１０は、複数のコンテンツの構成に対応する改竄検知情報として、複数のコンテンツを構成する各コンテンツのパス名（ディレクトリ名）を含むファイル名に対応したハッシュ値を改竄検知情報生成処理部１１１により生成し、ステップ２０２では、ステップ２０１で生成した改竄検知情報をＩＭ１０８に埋め込む。

【００２９】ステップ２０３でＩＭ生成処理部１１０は、複数のコンテンツの内容に対応する改竄検知情報として、複数のコンテンツを構成する各コンテンツデータ１０７の内容に対応したハッシュ値を改竄検知情報生成処理部１１１により生成する。ステップ２０４では、ステップ２０３で生成した改竄検知情報をＩＭ１０８に埋め込み、前記の様に複数のコンテンツの改竄検知情報が埋め込まれたＩＭ１０８をトップページに貼付ける。

【００３０】図３は本実施形態のパス名を含むファイル名に対応したハッシュ値の生成処理の概要を示す図である。図３に示す様にステップ２０１の処理では、改竄検知情報生成の対象となるコンテンツデータ１０７のパス名付きのファイル名３００を取得し、取得したファイル名３００の並びが一意に決定する様、取得したファイル名３００をアルファベット順等でソートした後、それらのファイル名３００のデータを連結してハッシュ値３２０を計算する。

【００３１】図４は本実施形態のパス名を含むファイル名に対応したハッシュ値の生成処理の処理手順を示すフローチャートである。図４に示す様にサーバ装置１００の改竄検知情報生成処理部１１１は、複数のコンテンツのパス名を含むファイル名に対応する改竄検知情報を生成する処理を行う。

【００３２】ステップ４０１で改竄検知情報生成処理部１１１は、改竄検知情報の生成の対象となるコンテンツを選択し、そのコンテンツデータ１０７のパス名付きのファイル名３００を取得する。例えばサーバ装置１００で公開しているホームページのトップページ以下に存在しているＨＴＭＬ(Hyper Text Markup Language)やＸＭＬ(eXtensible Markup Language)等のＷｅｂページを記述する為の記述言語で記載されたファイルやそれらのファイルにより表示される画像ファイルを選択したり、またトップページからリンクしているページの内でサーバ装置１００内に存在しているページのファイルそれらのファイルにより表示される画像ファイルを選択する。また改竄検知情報を生成するファイルを定義した生成情報を別途作成し、この生成情報に従ってサーバ装置１００中の特定のファイルについてのみ改竄検知情報を生成するものとしても良い。

【００３３】ステップ４０２では、ステップ４０１で取得したファイル名３００の並びが一意に決定する様、取得したファイル名３００をアルファベット順等でソートする。そしてステップ４０３では、それらのファイル名３００のデータを連結し、ステップ４０４では、前記連結したファイル名３００のデータについてのハッシュ値３２０を計算する。

【００３４】図５は本実施形態のコンテンツの内容に対応したハッシュ値の生成処理の概要を示す図である。図５に示す様にステップ２０３の処理では、先程取得したファイル名３１０のそれぞれについて、対応する実際のコンテンツデータ５００を取得する。更に、各コンテンツデータのハッシュ値５１０を計算する。次に、それらのハッシュ値５１０を連結し、それについてのハッシュ値５２０を計算する。

【００３５】図６は本実施形態のコンテンツの内容に対応したハッシュ値の生成処理の処理手順を示すフローチャートである。図６に示す様にサーバ装置１００の改竄検知情報生成処理部１１１は、複数のコンテンツのコンテンツデータに対応する改竄検知情報を生成する処理を行う。

【００３６】ステップ６０１で改竄検知情報生成処理部１１１は、先程取得したファイル名３１０のそれぞれについて、対応する実際のコンテンツデータ５００を取得し、ステップ６０２では、各コンテンツデータ５００のハッシュ値５１０を計算する。

【００３７】ステップ６０３では、各コンテンツデータ５００のハッシュ値５１０を連結し、ステップ６０４では、前記連結したハッシュ値５１０についてのハッシュ値５２０を計算する。

【００３８】前記の様にＩＭ１０８に埋め込んむファイル名３００のハッシュ値３２０及びコンテンツデータ５００のハッシュ値５２０は、コンテンツの改竄を検知する時に、正しい値として使用するものである。従って、コンテンツデータ５００の内容やファイル構成を変更した場合は、その都度、上記の通り各々のハッシュ値を計算し、ＩＭ１０８に埋め込み直す必要がある。但し、コンテンツデータ５００が変更される都度、ＩＭ１０８を自動生成し、コンテンツデータ５００に自動貼付するようなジェネレータを用意することで、利用者の操作を不要とすることも可能である。

【００３９】図７は本実施形態の改竄検知処理部１１２の処理手順を示すフローチャートである。図７に示す様にサーバ装置１００の改竄検知処理部１１２は、複数のコンテンツの登録または更新時の構成または内容に対応する改竄検知情報と、当該コンテンツの現在の構成または内容に対応する改竄検知情報とを比較して当該コンテ

ンツの改竄を検知する処理を行う。

【００４０】ステップ７０１で改竄検知処理部１１２は、図４に示した処理と同様にして複数のコンテンツを構成する各コンテンツについてそれらのパス名を含むファイル名に対するハッシュ値を改竄検知情報生成処理部１１１により計算する。

【００４１】ステップ７０２では、ＩＭ１０８内に埋め込まれているハッシュ値３２０と前記計算したハッシュ値の値とを比較し、ＩＭ１０８内に埋め込まれているハッシュ値３２０が前記計算したハッシュ値と異なる場合にはステップ７０３へ進む。

【００４２】前記パス名を含むファイル名に対するハッシュ値の相違は、コンテンツデータ１０７のファイル構成の改竄(コンテンツデータ１０７の削除・追加等)が行われたことを表している。従ってステップ７０３では、ファイル構成の改竄が行われたことを示す改竄通告を行う。改竄通告の方法としては、例えばシステム管理者のコンソール画面にメッセージを表示したり、或いは閲覧者がコンテンツのトップページを参照した時、ＩＭ１０８の画像デザインを変更し、コンテンツの改竄がなされていることを示す等が考えられる。

【００４３】ステップ７０４では、図６で示した処理と同様にして複数のコンテンツを構成する各コンテンツについてそれらの各コンテンツデータ５００に対するハッシュ値を改竄検知情報生成処理部１１１により計算する。

【００４４】ステップ７０５では、ＩＭ１０８内に埋め込まれているハッシュ値５２０と前記計算したハッシュ値の値とを比較し、ＩＭ１０８内に埋め込まれているハッシュ値５２０が前記計算したハッシュ値と異なる場合にはステップ７０６へ進む。

【００４５】前記各コンテンツデータ５００に対するハッシュ値の相違は、コンテンツデータ５００のファイル内容の改竄(コンテンツの文章の一部変更等)が行われたことを表している。従って、ステップ７０６では、ファイル内容の改竄が行われたことを示す改竄通告を行う。

【００４６】本実施形態では、改竄を検知する為の元データとして、パス付きのファイル名及び実際のコンテンツデータを用いているが、これらに加え、ファイル属性、コンテンツに貼付されている各種データ、リンクされている他のコンテンツ等を含めても良い。また、改竄を検知する為の情報として、ディレクトリやファイルの更新日時等を用いても良い。

【００４７】本実施形態では、改竄検知情報としてハッシュ値を計算し、ＩＭに埋め込んでいるが、これはデータの容量を少なく抑えることが目的である。従ってハッシュ値を計算せず、パス付きファイル名のデータや各コンテンツデータをそのままＩＭに埋め込んでも良い。また、各コンテンツデータ５００のハッシュ値５１０をそのままＩＭに埋め込んだり、各コンテンツデータ５００

を連結し、それに対して計算したハッシュ値をＩＭに埋め込む形態も可能である（コンテンツデータを特定する情報が残る形態であれば良い）。

【００４８】本実施形態では、改竄検知情報をトップページのＩＭに格納したが、各コンテンツ毎にＩＭを貼付しても良い。また、改竄検知情報をＩＭに埋め込むのではなく、デジタル署名としたり或いは加工せずにそのままの状態で磁気ディスク装置１０３内に格納しても良い。

【００４９】本実施形態において改竄検知処理部１１２を起動させる際には、サーバ装置１００の管理者等の手により手動で起動させる以外に、定期的に自動起動させたり、メモリに常駐させて常時検知を行ったり、また、閲覧者がコンテンツデータを参照した時に自動起動させる等の処理を行っても良い。

【００５０】以上説明した様に本実施形態のコンテンツ改竄検知装置によれば、複数のコンテンツの構成または内容の改竄を検知するので、コンテンツの改竄を早期発見することが可能である。

（実施形態２）以下にＥＸＩＴゲートを用いて改竄検知情報の有無を検知すると共に改竄位置を特定する実施形態２のコンテンツ改竄検知装置について説明する。

【００５１】図８は本実施形態のコンテンツ改竄検知装置の概要を示す図である。図８に示す様に本実施形態の改竄検知システムは、サーバ装置８００と、ＥＸＩＴゲート装置８１０と、クライアント装置８２０とを有している。

【００５２】サーバ装置８００は、コンテンツの登録または更新時の内容に対応する改竄検知情報を埋め込んだＩＭを貼付してコンテンツを生成し、ＥＸＩＴゲート装置８１０を介してクライアント装置８２０へ当該コンテンツを送信する装置である。

【００５３】ＥＸＩＴゲート装置８１０は、クライアント装置８２０から要求されたコンテンツの改竄を検知する装置である。クライアント装置８２０は、ＥＸＩＴゲート装置８１０から受け取ったコンテンツの改竄を検知し、改竄の行われていないコンテンツを表示する装置である。

【００５４】図８に示す様に本実施形態では、サーバ装置８００とクライアント装置８２０との間にＥＸＩＴゲート装置８１０を設け、ＥＸＩＴゲート装置８１０にてＩＭの有無のチェックやＩＭを用いた改竄検知を行う。またクライアント装置８２０でのチェックを併用することにより、サーバ装置８００上またはサーバ装置８００からＥＸＩＴゲート装置８１０までの経路上、若しくはＥＸＩＴゲート装置８１０からクライアント装置８２０までの経路上で改竄が行われているかどうかをチェックする。

【００５５】図９は本実施形態のサーバ装置８００の概略構成を示す図である。図９に示す様に本実施形態のサ

ーバ装置８００は、ＣＰＵ９０１と、メモリ９０２と、磁気ディスク装置９０３と、入力装置９０４と、出力装置９０５と、ＣＤ－ＲＯＭ装置９０６と、コンテンツデータ９０７と、ＩＭ９０８と、生成情報９０９とを有している。

【００５６】ＣＰＵ９０１は、サーバ装置８００全体の動作を制御する装置である。メモリ９０２は、サーバ装置８００全体の動作を制御する際にその為の各種処理プログラムやデータをロードする記憶装置である。磁気ディスク装置９０３は、前記各種処理プログラムやデータを格納しておく記憶装置である。

【００５７】入力装置９０４は、コンテンツを登録したり更新する為の各種入力を行う装置である。出力装置９０５は、コンテンツの登録や更新に伴う各種出力を行う装置である。ＣＤ－ＲＯＭ装置９０６は、前記各種処理プログラムを記録したＣＤ－ＲＯＭの内容を読み出す装置である。

【００５８】コンテンツデータ９０７は、クライアント装置１２０からの要求に応じて公開されるページの内容を示すデータである。ＩＭ９０８は、コンテンツデータ９０７に対応する改竄検知情報を埋め込んだ画像データである。生成情報９０９は、コンテンツの改竄を検知する為の改竄検知情報が生成されたコンテンツを示すデータである。

【００５９】またサーバ装置８００は、ＩＭ生成処理部９１０と、改竄検知情報生成処理部９１１と、生成情報作成処理部９１２と、改竄通知受信処理部９１３とを有している。

【００６０】ＩＭ生成処理部９１０は、コンテンツの内容に対応する改竄検知情報を埋め込んだＩＭ９０８を生成する処理部である。改竄検知情報生成処理部９１１は、コンテンツの内容に対応する改竄検知情報を生成する処理部である。

【００６１】生成情報作成処理部９１２は、コンテンツの改竄を検知する為の改竄検知情報が生成されたコンテンツを示す生成情報９０９を作成する処理部である。改竄通知受信処理部９１３は、コンテンツの改竄が行われていることを示す通知をＥＸＩＴゲート装置８１０から受信する処理部である。

【００６２】サーバ装置８００をＩＭ生成処理部９１０、改竄検知情報生成処理部９１１、生成情報作成処理部９１２及び改竄通知受信処理部９１３として機能させる為のプログラムは、ＣＤ－ＲＯＭ等の記録媒体に記録され磁気ディスク等に格納された後、メモリにロードされて実行されるものとする。なお前記プログラムを記録する記録媒体はＣＤ－ＲＯＭ以外の他の記録媒体でも良い。

【００６３】図１０は本実施形態のＥＸＩＴゲート装置８１０の概略構成を示す図である。図１０に示す様に本実施形態のＥＸＩＴゲート装置８１０は、ＣＰＵ１００

１と、メモリ１００２と、磁気ディスク装置１００３と、入力装置１００４と、出力装置１００５と、ＣＤ－ＲＯＭ装置１００６とを有している。

【００６４】ＣＰＵ１００１は、ＥＸＩＴゲート装置８１０全体の動作を制御する装置である。メモリ１００２は、ＥＸＩＴゲート装置８１０全体の動作を制御する際にその為の各種処理プログラムやデータをロードする記憶装置である。

【００６５】磁気ディスク装置１００３は、前記各種処理プログラムやデータを格納しておく記憶装置である。入力装置１００４は、コンテンツの改竄を検知する為の各種入力を行う装置である。出力装置１００５は、コンテンツの改竄の検知に伴う各種出力を行う装置である。ＣＤ－ＲＯＭ装置１００６は、前記各種処理プログラムを記録したＣＤ－ＲＯＭの内容を読み出す装置である。

【００６６】またＥＸＩＴゲート装置８１０は、生成検査処理部１０１０と、存在検査処理部１０１１と、改竄検知情報生成処理部１０１２と、改竄検知処理部１０１３とを有している。

【００６７】生成検査処理部１０１０は、コンテンツの改竄を検知する為の改竄検知情報が生成されたコンテンツを示す生成情報９０９を参照し、クライアント装置８２０から要求されたコンテンツについて、その改竄を検知する為の改竄検知情報が生成済みであるかどうかを検査する処理部である。

【００６８】存在検査処理部１０１１は、クライアント装置８２０から要求されたコンテンツについて、そのコンテンツの改竄検知情報の有無を検査する処理部である。改竄検知情報生成処理部１０１２は、クライアント装置８２０から要求されたコンテンツの現在の内容に対応する改竄検知情報を生成する処理部である。

【００６９】改竄検知処理部１０１３は、当該コンテンツの登録または更新時の内容に対応する改竄検知情報と前記生成した改竄検知情報とを比較して当該コンテンツの改竄を検知した場合に、サーバ装置８００上またはサーバ装置８００からＥＸＩＴゲート装置８１０までの経路上での当該コンテンツの改竄を検知したことを当該コンテンツの要求元であるクライアント装置８２０、登録元及び更新元であるサーバ装置８００に通知する処理部である。

【００７０】ＥＸＩＴゲート装置８１０を生成検査処理部１０１０、存在検査処理部１０１１、改竄検知情報生成処理部１０１２及び改竄検知処理部１０１３として機能させる為のプログラムは、ＣＤ－ＲＯＭ等の記録媒体に記録され磁気ディスク等に格納された後、メモリにロードされて実行されるものとする。なお前記プログラムを記録する記録媒体はＣＤ－ＲＯＭ以外の他の記録媒体でも良い。

【００７１】図１１は本実施形態のクライアント装置８２０の概略構成を示す図である。図１１に示す様に本実

施形態のクライアント装置８２０は、ＣＰＵ１１０１と、メモリ１１０２と、磁気ディスク装置１１０３と、入力装置１１０４と、出力装置１１０５と、ＣＤ－ＲＯＭ装置１１０６とを有している。

【００７２】ＣＰＵ１１０１は、クライアント装置８２０全体の動作を制御する装置である。メモリ１１０２は、クライアント装置８２０全体の動作を制御する際にその為の各種処理プログラムやデータをロードする記憶装置である。

【００７３】磁気ディスク装置１１０３は、前記各種処理プログラムやデータを格納しておく記憶装置である。入力装置１１０４は、コンテンツを要求して表示する為の各種入力を行う装置である。出力装置１１０５は、コンテンツの要求に伴ってコンテンツを表示する装置である。ＣＤ－ＲＯＭ装置１１０６は、前記各種処理プログラムを記録したＣＤ－ＲＯＭの内容を読み出す装置である。

【００７４】またクライアント装置８２０は、改竄検知情報生成処理部１１１０と、改竄検知処理部１１１１とを有している。

【００７５】改竄検知情報生成処理部１１１０は、要求したコンテンツをＥＸＩＴゲート装置８１０から受け取り、そのコンテンツの現在の内容に対応する改竄検知情報を生成する処理部である。改竄検知処理部１１１１は、当該コンテンツの登録または更新時の内容に対応する改竄検知情報と前記生成した改竄検知情報とを比較して当該コンテンツの改竄を検知した場合に、ＥＸＩＴゲート装置８１０からクライアント装置８２０までの経路上での当該コンテンツの改竄を検知したことを示す表示を行う処理部である。

【００７６】クライアント装置８２０を改竄検知情報生成処理部１１１０及び改竄検知処理部１１１１として機能させる為のプログラムは、ＣＤ－ＲＯＭ等の記録媒体に記録され磁気ディスク等に格納された後、メモリにロードされて実行されるものとする。なお前記プログラムを記録する記録媒体はＣＤ－ＲＯＭ以外の他の記録媒体でも良い。

【００７７】図１２は本実施形態のコンテンツ登録／更新処理の処理手順を示すフローチャートである。図１２に示す様にサーバ装置８００では、登録や更新が行われたコンテンツの内容に対応する改竄検知情報を埋め込んだＩＭ９０８を生成して当該コンテンツに貼付けた後、ＩＭ９０８の貼付けが行われたコンテンツを示す生成情報９０９を作成する処理を行う。

【００７８】ステップ１２０１でＩＭ生成処理部９１０は、コンテンツデータ９０７の登録や更新が行われたかどうかを調べ、コンテンツデータ９０７の登録や更新が行われている場合にはステップ１２０２へ進む。

【００７９】ステップ１２０２では、登録や更新が行われたコンテンツについて、そのコンテンツデータ９０７

のハッシュ値を改竄検知情報生成処理部９１１により計算し、その内容に対応する改竄検知情報としてＩＭ９０８に埋め込む。そしてステップ１２０３では、ステップ１２０２で改竄検知情報を埋め込んだＩＭ９０８を、前記登録や更新が行われたコンテンツに貼付ける。

【００８０】ステップ１２０４で生成情報作成処理部９１２は、ステップ１２０３でＩＭ９０８の貼付けが行われたコンテンツを示す情報を生成情報９０９に設定し、ステップ１２０５では、前記設定した生成情報９０９をＥＸＩＴゲート装置８１０へ送る。

【００８１】図１３は本実施形態の生成情報９０９の一例を示す図である。図１３に示す様に生成情報９０９には、ＩＭ９０８の貼付けが行われたコンテンツを示す情報として、ＩＭ９０８の貼付けが行われたコンテンツデータ９０７のパス名を含むファイル名や貼付けられたＩＭ９０８の生成日付時刻等の情報が設定されている。

【００８２】図１４は本実施形態のクライアント側処理の処理手順を示すフローチャートである。図１４に示す様にクライアント装置８２０は、要求したコンテンツをＥＸＩＴゲート装置８１０から受け取り、そのコンテンツの現在の内容に対応する改竄検知情報を生成して改竄を検知する処理を行う。

【００８３】ステップ１４０１でクライアント装置８２０のWWWブラウザは、ユーザがＵＲＬ(Uniform Resource Locators)を入力したかどうかを調べ、ユーザがＵＲＬを入力した場合にはそのＵＲＬを受付けてステップ１４０２へ進む。ステップ１４０２では、ステップ１４０１で受付けたＵＲＬのページを表示する為のリクエストを前記ＵＲＬで示される宛先へ送信する。前記ＵＲＬで示される宛先がサーバ装置８００であり、その経路上にＥＸＩＴゲート装置８１０がある場合には、前記リクエストはＥＸＩＴゲート装置８１０を経由してサーバ装置８００へ送られる。

【００８４】ステップ１４０３では、前記送信したリクエストの結果としてＨＴＭＬデータを受信しているかどうかを調べ、ＨＴＭＬデータを受信している場合にはステップ１４０４へ進む。

【００８５】ステップ１４０４では、ステップ１４０３で受信したＨＴＭＬデータ中にＩＭ９０８が貼付けられているかどうかを調べ、ＩＭ９０８が貼付けられている場合にはステップ１４０５へ進み、ＩＭ９０８が貼付けられていない場合にはステップ１４０６へ進む。

【００８６】ステップ１４０５で改竄検知処理部１１１１は、ステップ１４０３で受信したＨＴＭＬデータについて、その内容に対するハッシュ値を改竄検知情報生成処理部１１１０により計算し、ＩＭ９０８中のハッシュ値と前記計算したハッシュ値とを比較して当該コンテンツの改竄が行われているかどうかを調べる。当該コンテンツの改竄が行われているかどうかを調べた結果、当該コンテンツの改竄が検知されない場合にはステップ１４

０６へ進み、当該コンテンツの改竄を検知した場合にはステップ１４０７へ進む。

【００８７】ステップ１４０６では、ステップ１４０３で受信したＨＴＭＬデータに従ってページを表示する。ここで前記ＵＲＬのリクエストを処理する際にＥＸＩＴゲート装置８１０が当該ページの改竄を検知した場合には、改竄が検知されたことを示すＨＴＭＬデータがＥＸＩＴゲート装置８１０から送られてきているので、クライアント装置８２０では当該ページの改竄がＥＸＩＴゲート装置８１０で検知されたことを示す表示が行われる。

【００８８】ステップ１４０７では、ステップ１４０３で受信したＨＴＭＬデータ中にＥＸＩＴゲート装置８１０での処理が行われたことを示す情報が含まれているかを調べ、ＥＸＩＴゲート装置８１０での処理が行われたことを示す情報が含まれている場合にはステップ１４０８へ進み、含まれていない場合にはステップ１４０９へ進む。

【００８９】ステップ１４０８では、ＥＸＩＴゲート装置８１０からクライアント装置８２０までの経路上での当該コンテンツの改竄を検知したことを示す表示を行い、ステップ１４０９では、単に当該コンテンツの改竄を検知したことを示す表示を行う。

【００９０】図１５は本実施形態のＥＸＩＴゲート側処理の処理手順を示すフローチャートである。ステップ１５０１でＥＸＩＴゲート装置８１０の改竄検知処理部１０１３は、クライアント装置８２０からリクエストを受信しているかどうかを調べ、リクエストを受信している場合にはステップ１５０２へ進む。

【００９１】ステップ１５０２では、当該リクエストで要求されているコンテンツデータ９０７をキャッシュとして保持しているかどうかを調べ、保持していない場合にはステップ１５０３で当該リクエストをサーバ装置８００へ送る。

【００９２】ステップ１５０４では、当該リクエストに対応するＨＴＭＬデータをサーバ装置８００から受信しているかどうかを調べ、ＨＴＭＬデータを受信している場合にはステップ１５０５へ進む。

【００９３】ステップ１５０５で生成検査処理部１０１０は、コンテンツの改竄を検知する為の改竄検知情報が生成されたコンテンツを示す生成情報９０９を参照する。ステップ１５０６では、クライアント装置８２０から要求されたコンテンツについて、その改竄を検知する為の改竄検知情報が生成済みであるかどうかを調べ、改竄検知情報が生成済みである場合にはステップ１５０７へ進む。

【００９４】ステップ１５０７で存在検査処理部１０１１は、ステップ１５０４で受信したＨＴＭＬデータ中に生成情報９０９で示されたＩＭ９０８が貼付けられているかどうかを調べ、クライアント装置８２０から要求されたコンテンツについて、そのコンテンツの改竄検知情報の有無を検査する処理を行う。生成情報９０９で示されたＩＭ９０８が貼付けられている場合にはステップ１５０８へ進み、生成情報９０９で示されたＩＭ９０８が貼付けられていない場合にはステップ１５１１へ進む。

【００９５】ステップ１５０８で改竄検知処理部１０１３は、ステップ１５０４で受信したＨＴＭＬデータについて、その内容に対するハッシュ値を改竄検知情報生成処理部１０１２により計算し、ＩＭ９０８中のハッシュ値と前記計算したハッシュ値とを比較して当該コンテンツの改竄が行われているかどうかを調べる。当該コンテンツの改竄が行われているかどうかを調べた結果、当該コンテンツの改竄が検知されない場合にはステップ１５０９へ進み、当該コンテンツの改竄を検知した場合にはステップ１５１２へ進む。

【００９６】ステップ１５０９では、ステップ１５０４で受信したＨＴＭＬデータであるコンテンツデータ９０７をキャッシュとして保持し、ステップ１５１０では、ＥＸＩＴゲート装置８１０での処理が行われたことを示す情報と共に当該ＨＴＭＬデータをクライアント装置８２０へ送信する。

【００９７】ステップ１５１１では、サーバ装置８００上またはサーバ装置８００からＥＸＩＴゲート装置８１０までの経路上での当該コンテンツの改竄検知情報の除去を検知したことを示す表示を行う。またステップ１５１２では、サーバ装置８００上またはサーバ装置８００からＥＸＩＴゲート装置８１０までの経路上での当該コンテンツの内容の改竄を検知したことを示す表示を行う。

【００９８】ステップ１５１３では、当該コンテンツの登録元及び更新元であるサーバ装置８００に、サーバ装置８００上またはサーバ装置８００からＥＸＩＴゲート装置８１０までの経路上で、当該コンテンツの改竄検知情報の除去または当該コンテンツの内容の改竄が行われたことを通知する処理を行う。

【００９９】またステップ１５１３では、当該コンテンツの要求元であるクライアント装置８２０に、サーバ装置８００上またはサーバ装置８００からＥＸＩＴゲート装置８１０までの経路上で、当該コンテンツの改竄検知情報の除去または当該コンテンツの内容の改竄が行われたことを通知する処理を行う。

【０１００】図１６は本実施形態の改竄通知受信処理部９１３の処理手順を示すフローチャートである。図１６に示す様にサーバ装置８００の改竄通知受信処理部９１３は、コンテンツの改竄が行われていることを示す通知をＥＸＩＴゲート装置８１０から受信する処理を行う。

【０１０１】ステップ１６０１で改竄通知受信処理部９１３は、コンテンツの改竄が行われていることを示す通知をＥＸＩＴゲート装置８１０から受信しているかどうかを調べ、コンテンツの改竄が行われていることを示す

15

通知を受信している場合にはステップ１６０２へ進む。ステップ１６０２では、受信した通知内容を表示してサーバ装置８００の管理者に知らせ、ステップ１６０３では、受信した通知内容を磁気ディスク装置９０３に格納する。

【０１０２】以上説明した様に本実施形態のコンテンツ改竄検知装置によれば、改竄検知情報の有無を検査するので、改竄検知情報の除去による改竄の隠蔽を防止することが可能である。

【０１０３】また本実施形態のコンテンツ改竄検知装置によれば、クライアントとサーバの間でコンテンツの改竄を検知するので、改竄が行われた位置を特定することが可能である。

【０１０４】

【発明の効果】本発明によれば複数のコンテンツの構成または内容の改竄を検知するので、コンテンツの改竄を早期発見することが可能である。

【図面の簡単な説明】

【図１】実施形態１のコンテンツ改竄検知装置の概略構成を示す図である。

【図２】実施形態１のＩＭ生成処理部１１０の処理手順を示すフローチャートである。

【図３】実施形態１のパス名を含むファイル名に対応したハッシュ値の生成処理の概要を示す図である。

【図４】実施形態１のパス名を含むファイル名に対応したハッシュ値の生成処理の処理手順を示すフローチャートである。

【図５】実施形態１のコンテンツの内容に対応したハッシュ値の生成処理の概要を示す図である。

【図６】実施形態１のコンテンツの内容に対応したハッシュ値の生成処理の処理手順を示すフローチャートである。

【図７】実施形態１の改竄検知処理部１１２の処理手順を示すフローチャートである。

【図８】実施形態２のコンテンツ改竄検知装置の概要を示す図である。

【図９】実施形態２のサーバ装置８００の概略構成を示す図である。

【図１０】実施形態２のＥＸＩＴゲート装置８１０の概略構成を示す図である。

16

【図１１】実施形態２のクライアント装置８２０の概略構成を示す図である。

【図１２】実施形態２のコンテンツ登録／更新処理の処理手順を示すフローチャートである。

【図１３】実施形態２の生成情報９０９の一例を示す図である。

【図１４】実施形態２のクライアント側処理の処理手順を示すフローチャートである。

【図１５】実施形態２のＥＸＩＴゲート側処理の処理手順を示すフローチャートである。

【図１６】実施形態２の改竄通知受信処理部９１３の処理手順を示すフローチャートである。

【符号の説明】

１００…サーバ装置、１２０…クライアント装置、１０１…ＣＰＵ、１０２…メモリ、１０３…磁気ディスク装置、１０４…入力装置、１０５…出力装置、１０６…ＣＤ－ＲＯＭ装置、１０７…コンテンツデータ、１０８…ＩＭ、１１０…ＩＭ生成処理部、１１１…改竄検知情報生成処理部、１１２…改竄検知処理部、３００及び３１０…ファイル名、３２０…ハッシュ値、５００…コンテンツデータ、５１０及び５２０…ハッシュ値、８００…サーバ装置、８１０…ＥＸＩＴゲート装置、８２０…クライアント装置、９０１…ＣＰＵ、９０２…メモリ、９０３…磁気ディスク装置、９０４…入力装置、９０５…出力装置、９０６…ＣＤ－ＲＯＭ装置、９０７…コンテンツデータ、９０８…ＩＭ、９０９…生成情報、９１０…ＩＭ生成処理部、９１１…改竄検知情報生成処理部、９１２…生成情報作成処理部、９１３…改竄通知受信処理部、１００１…ＣＰＵ、１００２…メモリ、１００３…磁気ディスク装置、１００４…入力装置、１００５…出力装置、１００６…ＣＤ－ＲＯＭ装置、１０１０…生成検査処理部、１０１１…存在検査処理部、１０１２…改竄検知情報生成処理部、１０１３…改竄検知処理部、１１０１…ＣＰＵ、１１０２…メモリ、１１０３…磁気ディスク装置、１１０４…入力装置、１１０５…出力装置、１１０６…ＣＤ－ＲＯＭ装置、１１１０…改竄検知情報生成処理部、１１１１…改竄検知処理部。

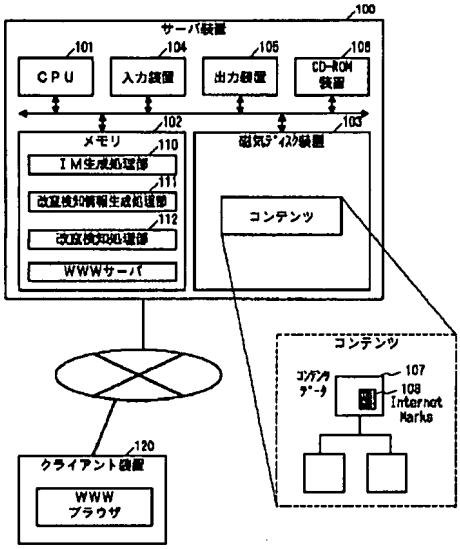
【図１３】

図１３

ファイル名	日付時刻	…
index.html	2000/3/28 11:06	…
downlcontent2.html	2000/3/28 11:16	…
:	:	…

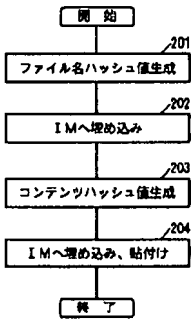
【図１】

図１



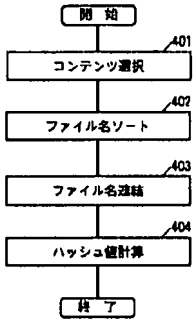
【図２】

図２



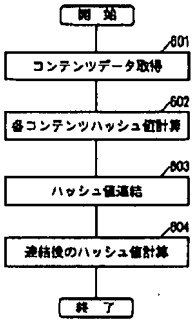
【図４】

図４



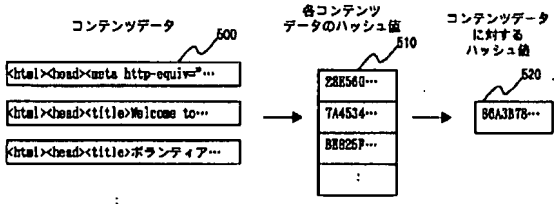
【図６】

図６



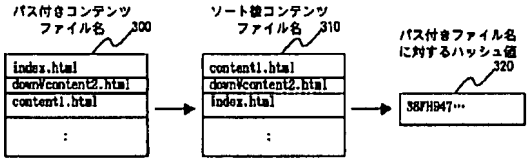
【図５】

図５



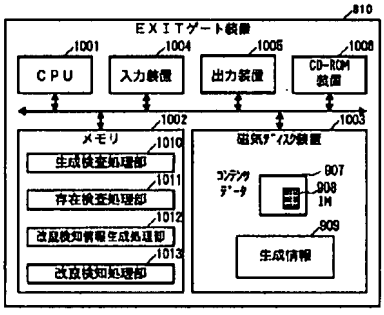
【図３】

図３



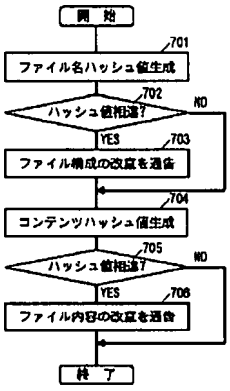
【図１０】

図１０



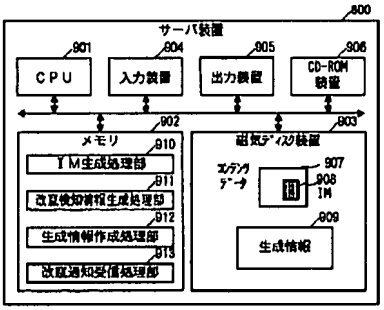
【図７】

図７



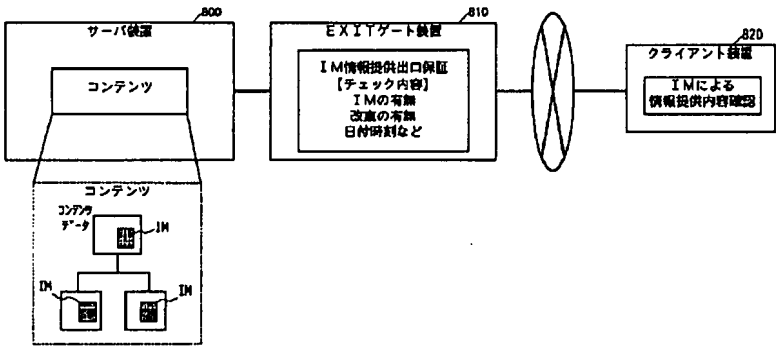
【図９】

図９



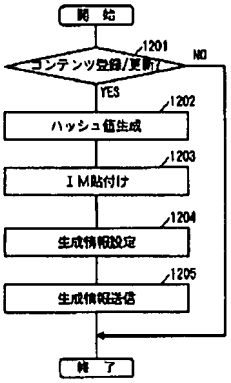
【図８】

図８



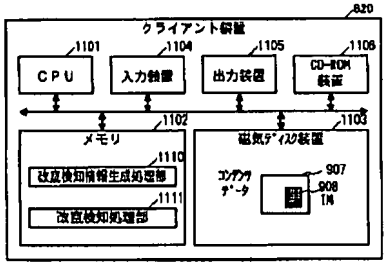
【図１２】

図１２



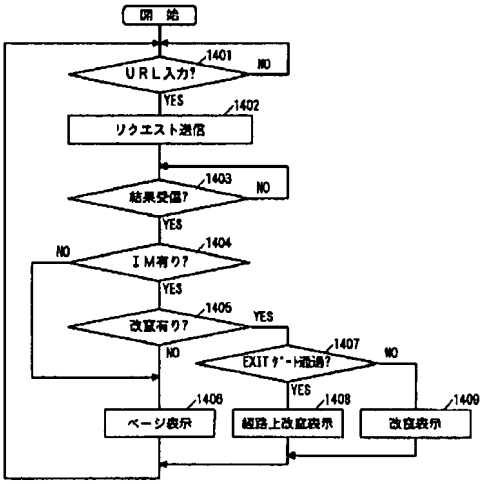
【図１１】

図１１



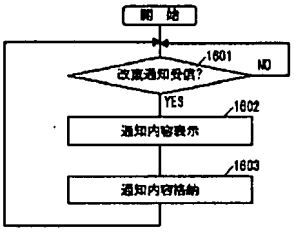
【図１４】

図１４



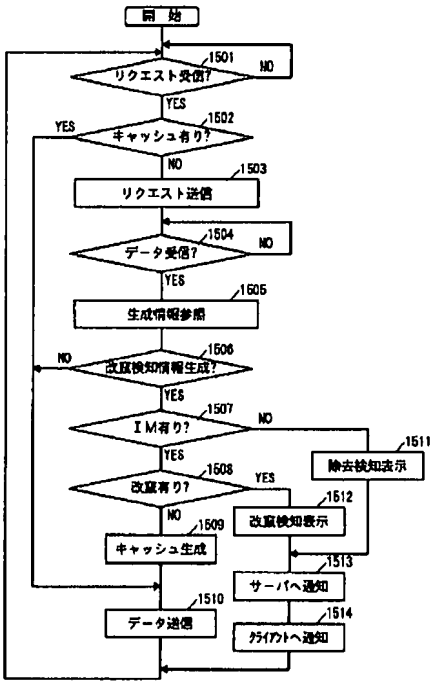
【図１６】

図１６



【図１５】

図１５



フロントページの続き

(72)発明者　中島　純三
東京都江東区新砂一丁目６番27号　株式会
社日立製作所公共システム事業部内

Ｆターム(参考)　5B017 AA02 BA09 CA15 CA16
5B085 AA08 AE15 AE29 BA06
5J104 AA08 LA01 NA12 PA07
9A001 JJ25 JJ27 LL03

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2001-282619

(43)Date of publication of application : 12.10.2001

(51)Int.Cl. G06F 12/14
G06F 15/00
G09C 1/00

(21)Application number : 2000-094313

(22)Date of filing : 30.03.2000

(71)Applicant : HITACHI LTD

(72)Inventor : SHINODA TAKASHI
TOYOSHIMA HISASHI
NAKAJIMA JUNZO

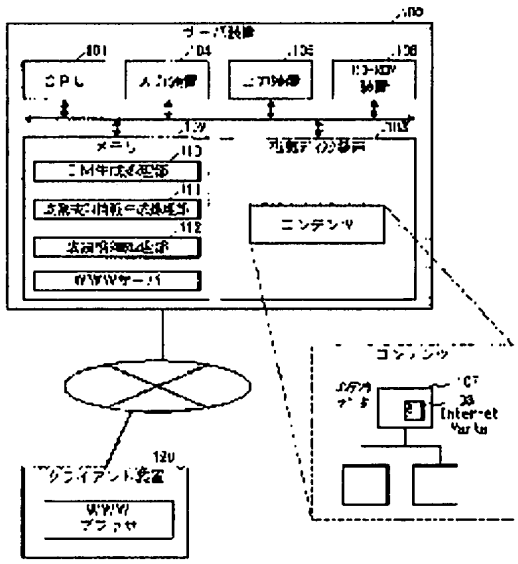
(54) METHOD AND DEVICE FOR DETECTING CONTENT ALTERATION AND RECORDING MEDIUM WITH RECORDED PROCESSING PROGRAM THEREON

(57)Abstract:

PROBLEM TO BE SOLVED: To provide technology which can find alteration of contents at an early stage.

SOLUTION: The content alteration detecting method for detecting alteration of contents has a step for generating alteration detection information, corresponding to the current constitution or contents of plural contents and a step for detecting the alteration of the contents by comparing the alteration detection information, corresponding to the constitution or contents at registration or update of the contents with the generated alteration detection information.

図 1



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

* NOTICES *

1.This document has been translated by computer. So the translation may not reflect the original precisely.
2.**** shows the word which can not be translated.
3.In the drawings, any words are not translated.

CLAIMS

[Claim(s)]
[Claim 1] The contents alteration detection approach of carrying out having the step which compares the step which generates the alteration detection information corresponding to two or more the current configurations or contents of contents with the alteration detection information corresponding to a configuration or the contents and said generated alteration detection information at the time of registration of the contents concerned, or updating in the contents alteration detection approach which detects the alteration of contents, and detects the alteration of the contents concerned as the description.
[Claim 2] The contents alteration detection approach characterized by having the step which inspects whether the alteration detection information for detecting the alteration about a certain contents is generation ending in the contents alteration detection approach which detects the alteration of contents, and the step which inspects the existence of the alteration detection information on the contents concerned.
[Claim 3] The contents alteration detection approach of carrying out having the step notify to the demand origin of the contents concerned, a registering agency, or an updating agency when the step which generates the alteration detection information corresponding to the current contents of contents compares with the alteration detection information corresponding to the contents and said alteration detection information which generated at the time of registration of the contents concerned, or updating in the contents alteration detection approach which detects the alteration of contents and the alteration of the contents concerned detects as the description.
[Claim 4] The contents alteration detection equipment carry out having the alteration detection processing [of comparing the alteration detection information generation processing section which generates the alteration detection information corresponding to two or more the current configurations or contents of contents, and the alteration detection information corresponding to a configuration or the contents and said alteration detection information which generated at the time of registration of the contents concerned, or updating in the contents alteration detection equipment which detects the alteration of contents, and detecting the alteration of the contents concerned] section as the description.
[Claim 5] In the record medium which recorded the program for operating a computer as contents alteration detection equipment which detects the alteration of contents and in which computer reading is possible The alteration detection information generation processing section which generates the alteration detection information corresponding to two or more the current configurations or contents of contents, The record medium characterized by recording the program for operating a computer as the alteration detection processing section which compares the alteration detection information corresponding to a configuration or the contents and said generated alteration detection information at the time of registration of the contents concerned, or updating, and detects the alteration of the contents concerned.

[Translation done.]

* NOTICES *

DETAILED DESCRIPTION

[Detailed Description of the Invention]
[0001]
[Field of the Invention] This invention is applied to the contents alteration detection equipment which detects the alteration performed to the contents displayed especially by the homepage of the Internet about the contents alteration detection equipment which detects the alteration of contents, and relates to an effective technique.
[0002]
[Description of the Prior Art] Conventionally, government and municipal offices, many companies, etc. open a homepage to WWW (World Wide Web) server equipment, and that including an individual are performing various kinds of information dispatch. It is going across the contents exhibited by the homepage which government and municipal offices and a company open variably from the easy information to the thing of contents equivalent to an official announcement, and anyone can acquire such information now by accessing the Internet.
[0003] The contents of the homepage which these government and municipal offices and companies open may cause the remarkable fall of trust, when an error is in the contents or the contents of the homepage are altered by the unauthorized entry to the server by external human being, since it is thought that the government and municipal offices and company are sending to the forward type to the exterior. Although it is necessary to fully take those security countermeasures even if it is the case where the homepage is opened for an easy public service campaign for this reason, in recent years, external human being accesses servers, such as government and municipal offices, illegally, and there have been a lot of incidents in which the contents of the homepage are altered.
[0004] In addition, while enabling authentication of the bona fides of strict electronic data, the generation method of the electronic data which expresses the bona fides to the user of electronic data visually and which can be attested is indicated by JP,2000-78125,A. The outline embeds the electronic mark A which expresses bona fides visually as visible digital watermarking to the electronic mark B, after embedding what added the digital signature to the authentication information for attesting the electronic marks B, such as a Web page and a trademark, as invisible digital watermarking to the electronic mark A.
[0005]
[Problem(s) to be Solved by the Invention] Since the big problem in the incident which has the contents of the above homepages altered has the huge amount of the homepage which the security countermeasures of the server which exhibits a homepage exhibit [being sweet], even if some homepages are altered, it is in the point that it tends to be overdue to notice it.
[0006] The purpose of this invention solves the above-mentioned problem, and it is in offering the technique which can carry out early detection of the alteration of contents.
[0007] Other purposes of this invention are to offer the technique which can prevent concealment of the alteration by removal of alteration detection information.
[0008] Other purposes of this invention are to offer the technique which can pinpoint the location in.
[0009]
[Means for Solving the Problem] This invention detects the configuration of two or more contents, or the alteration of the contents in the contents alteration detection equipment which detects the alteration of contents.
[0010] In this invention, the alteration detection information corresponding to those configurations or

contents is generated at the time of registration of two or more contents, or updating. And when predetermined conditions, like predetermined time of day comes are satisfied, after generating the alteration detection information corresponding to the current configuration or the current contents of the contents concerned with reference to said generated alteration detection information, said alteration detection information referred to is compared with said generated alteration detection information, the alteration of the contents concerned is detected, and the alteration of the contents concerned is notified.
[0011] For example, at the time of registration of two or more contents displayed by the homepage currently exhibited, or updating, the hash value of those file structures and contents of each file is generated as alteration detection information, it embeds at IM (Internet-Marks), and the IM is stuck on the top page of a homepage.
[0012] And when predetermined conditions, like predetermined time of day comes by processing of a resident program etc. are satisfied, with reference to the hash value of the registration in said stuck IM, or the file structure at the time of updating and the contents of each file, hash count of current file organization or the contents of each file is performed. Next, the hash value of the registration in said IM referred to, or the file structure at the time of updating and the contents of each file is compared with the hash value of said generated current file structure and contents of each file, and a visitor is told about having changed the design of IM of a top page and the alteration of contents having been performed, while notifying the system administrator, when said generated current hash value differed from the hash value currently embedded at IM.
[0013] As mentioned above, in this invention, even if human beings, such as a system administrator, do not always check, when a part of homepage currently exhibited is altered, it becomes possible to notify immediately that the alteration was performed, and unjust early detection can be performed. Moreover, it becomes possible to tell immediately that the alteration of a homepage was performed to coincidence also to the visitor.
[0014] Since the configuration of two or more contents or the alteration of the contents is detected as mentioned above according to the contents alteration detection equipment of this invention, it is possible to carry out early detection of the alteration of contents.
[0015]
[Embodiment of the Invention] (Operation gestalt 1) The contents alteration detection equipment of the operation gestalt 1 which detects the alteration of two or more contents is explained below.
[0016] Drawing 1 is drawing showing the outline configuration of the contents alteration detection equipment of this operation gestalt. As shown in drawing 1 , the server equipment 100 of this operation gestalt has CPU101, memory 102, a magnetic disk drive 103, an input device 104, an output unit 105, CD-ROM equipment 106, the contents data 107, and IM108.
[0017] CPU101 is equipment which controls actuation of the server equipment 100 whole. In case memory 102 controls actuation of the server equipment 100 whole, it is storage which loads the various processing programs and data for it. A magnetic disk drive 103 is storage which stores said various processing programs and data.
[0018] An input unit 104 is equipment which performs the various inputs for detecting the alteration of two or more contents. An output unit 105 is equipment which performs the various outputs accompanying detection of an alteration of two or more contents. CD-ROM equipment 106 is equipment which reads the contents of the CD-ROM which recorded said various processing programs.
[0019] The contents data 107 are data in which the contents of the page exhibited according to the demand from client equipment 120 are shown. IM108 is the image data which embedded the alteration detection information corresponding to two or more contents data 107.
[0020] Moreover, server equipment 100 has IM generation processing section 110, the alteration detection information generation processing section 111, and the alteration detection processing section 112.
[0021] IM generation processing section 110 is the processing section which generates IM which embedded the alteration detection information corresponding to the configuration or the contents at the time of registration of two or more contents, or updating. The alteration detection information generation processing section 111 is the processing section which generates the alteration detection information corresponding to two or more configurations or contents of contents.
[0022] The alteration detection processing section 112 is the processing section which compares the alteration detection information corresponding to the configuration or the contents at the time of registration of two or more contents, or updating with the alteration detection information corresponding

to the current configuration or the current contents of the contents concerned, and detects the alteration of the contents concerned.
[0023] After being recorded on record media, such as CD-ROM, and being stored in a magnetic disk etc., the program for operating server equipment 100 as IM generation processing section 110, the alteration detection information generation processing section 111, and the alteration detection processing section 112 shall be loaded to memory, and shall be performed. In addition, other record media other than CD-ROM are sufficient as the record medium which records said program.
[0024] Let mutually the server equipment 100 which manages and exhibits contents data, and the client equipment 120 which peruses contents data be the things which can transmit and receive data by networks, such as the Internet.
[0025] The WWW server which exhibits contents data according to the demand from client equipment 120 is mounted in server equipment 100, and the WWW browser which receives and displays contents data is mounted in client equipment 120 from server equipment.
[0026] Moreover, two or more contents data 107 are stored in the magnetic disk drive 103 connected to server equipment 100, and suppose that IM108 which is the Internet mark which embedded the alteration detection information corresponding to two or more contents data 107 one of them, for example, the top page of contents, is stuck.
[0027] Drawing 2 is a flow chart which shows the procedure of IM generation processing section 110 of this operation gestalt. As shown in drawing 2 , IM generation processing section 110 of server equipment 100 performs processing which generates IM which embedded the alteration detection information corresponding to the configuration or the contents at the time of registration of two or more contents, or updating.
[0028] At step 201, IM generation processing section 110 generates the hash value corresponding to the file name containing the pathname (directory name) of each contents which constitute two or more contents as alteration detection information corresponding to the configuration of two or more contents by the alteration detection information generation processing section 111, and embeds the alteration detection information generated at step 201 in step 202 at IM108.
[0029] IM generation processing section 110 generates the hash value corresponding to the contents of each contents data 107 which constitutes two or more contents as alteration detection information corresponding to the contents of two or more contents by the alteration detection information generation processing section 111 at step 203. At step 204, IM108 where the alteration detection information generated at step 203 was embedded at IM108, and the alteration detection information on two or more contents was embedded as mentioned above is stuck on a top page.
[0030] Drawing 3 is drawing showing the outline of generation processing of the hash value corresponding to the file name containing the pathname of this operation gestalt. As shown in drawing 3 , after the list of the file name 300 which acquired the file name 300 with the pathname of the contents data 107 set as the object of alteration detection information generation by processing of step 201, and was acquired sorts the appearance determined as a meaning, and the acquired file name 300 in an alphabetical order etc., a hash value 320 is calculated by connecting the data of those file names 300.
[0031] Drawing 4 is a flow chart which shows the procedure of generation processing of the hash value corresponding to the file name containing the pathname of this operation gestalt. As shown in drawing 4 , the alteration detection information generation processing section 111 of server equipment 100 performs processing which generates the alteration detection information corresponding to the file name containing the pathname of two or more contents.
[0032] At step 401, the alteration detection information generation processing section 111 chooses the contents set as the object of generation of alteration detection information, and acquires the file name 300 with the pathname of the contents data 107. for example, the file of the page which exists in server equipment 100 among the pages which choose the image file displayed by the files indicated by the description language for describing Web pages which exist below in the top page of the homepage currently exhibited with server equipment 100, such as HTML (Hyper Text Markup Language) and XML (eXtensible Markup Language), and those files, and are linked from the top page -- the image file displayed by the file of them chooses. Moreover, it is good also as what creates separately the creation information which defined the file which generates alteration detection information, and generates alteration detection information only about the specific file in server equipment 100 according to this creation information.
[0033] In step 402, the list of the file name 300 acquired at step 401 sorts the appearance determined as a

meaning, and the acquired file name 300 in an alphabetical order etc. And the data of those file names 300 are connected at step 403, and the hash value 320 about said connected data of a file name 300 is calculated at step 404.

[0034] Drawing 5 is drawing showing the outline of generation processing of the hash value corresponding to the contents of the contents of this operation gestalt. As shown in drawing 5 , in processing of step 203, the actual corresponding contents data 500 are acquired about each of the file name 310 acquired previously. Furthermore, the hash value 510 of each contents data is calculated. Next, those hash values 510 are connected and the hash value 520 about it is calculated.

[0035] Drawing 6 is a flow chart which shows the procedure of generation processing of the hash value corresponding to the contents of the contents of this operation gestalt. As shown in drawing 6 , the alteration detection information generation processing section 111 of server equipment 100 performs processing which generates the alteration detection information corresponding to the contents data of two or more contents.

[0036] About each of the file name 310 which acquired the alteration detection information generation processing section 111 previously at step 601, the actual corresponding contents data 500 are acquired and the hash value 510 of each contents data 500 is calculated at step 602.

[0037] At step 603, the hash value 510 of each contents data 500 is connected, and the hash value 520 about said connected hash value 510 is calculated at step 604.

[0038] It buries to IM108 as mentioned above, and the hash value 320 of the ****** file name 300 and the hash value 520 of the contents data 500 are used as a right value, when detecting the alteration of contents. Therefore, when the contents and file organization of the contents data 500 are changed, each hash value is calculated as above-mentioned, and it is necessary to reembed at IM108 each time. However, whenever the contents data 500 are changed, it is also possible to generate IM108 automatically and to make actuation of a user unnecessary by preparing a generator which carries out automatic pasting at the contents data 500.

[0039] Drawing 7 is a flow chart which shows the procedure of the alteration detection processing section 112 of this operation gestalt. As shown in drawing 7 , the alteration detection processing section 112 of server equipment 100 performs processing which compares the alteration detection information corresponding to the configuration or the contents at the time of registration of two or more contents, or updating with the alteration detection information corresponding to the present configuration or the present contents of the contents concerned, and detects the alteration of the contents concerned.

[0040] The alteration detection processing section 112 calculates the hash value to the file name which contains those pathnames about each contents which constitute two or more contents like the processing shown in drawing 4 by the alteration detection information generation processing section 111 at step 701.

[0041] At step 702, the hash value 320 currently embedded in IM108 is compared with said calculated value of a hash value, and when the hash value 320 currently embedded in IM108 differs from said calculated hash value, it progresses to step 703.

[0042] The difference of the hash value to the file name containing said pathname means that the alterations (deletion, addition, etc. of the contents data 107) of the file organization of the contents data 107 were performed. Therefore, at step 703, alteration announcement which shows that the alteration of file organization was performed is performed. When a message is displayed, for example on a system administrator's console screen or a visitor refers to the top page of contents as the approach of alteration announcement, the image design of IM108 is changed and it is possible that it is shown that the alteration of contents is made etc.

[0043] The hash value to each of those contents data 500 is calculated by the alteration detection information generation processing section 111 about each contents which constitute two or more contents from a step 704 like the processing shown by drawing 6 .

[0044] At step 705, the hash value 520 currently embedded in IM108 is compared with said calculated value of a hash value, and when the hash value 520 currently embedded in IM108 differs from said calculated hash value, it progresses to step 706.

[0045] The difference of the hash value to said each contents data 500 means that the alterations (partial change of the text of contents etc.) of the file content of the contents data 500 were performed. Therefore, at step 706, alteration announcement which shows that the alteration of a file content was performed is performed.

[0046] With this operation gestalt, as former data for detecting an alteration, although a file name and

actual contents data with pass are used, in addition to these, a file attribute, the various data stuck on contents, other contents linked may be included. Moreover, a directory, the updating time of a file, etc. may be used as information for detecting an alteration.
[0047] Although a hash value is calculated as alteration detection information and embedded with this operation gestalt at IM, it is the purpose that this stops the capacity of data few. Therefore, you may not calculate a hash value but may also embed data and each contents data of a file name with pass as it is at IM. Moreover, the gestalt which embeds at IM the hash value which embedded the hash value 510 of each contents data 500 as it was at IM, or connected each contents data 500, and was calculated to it is also possible (what is necessary is just the gestalt in which the information which specifies contents data remains).
[0048] With this operation gestalt, although alteration detection information was stored in IM of a top page, IM may be stuck for every contents. Moreover, alteration detection information is not embedded at IM, but it may consider as a digital signature or you may store in a magnetic disk drive 103 in the condition as it is, without processing it.
[0049] In case the alteration detection processing section 112 is started in this operation gestalt, when it was made to reside in memory permanently, and it always detects and a visitor refers to [**** / carrying out auto-boot periodically] contents data in addition to making it start manually by hands, such as a manager of server equipment 100, you may process carrying out auto-boot etc.
[0050] Since the configuration of two or more contents or the alteration of the contents is detected like according to the contents alteration detection equipment of this operation gestalt, the thing which were explained above and to do for the early detection of the alteration of contents is possible.
(Operation gestalt 2) While using the EXIT gate for below and detecting the existence of alteration detection information, the contents alteration detection equipment of the operation gestalt 2 which pinpoints an alteration location is explained.
[0051] Drawing 8 is drawing showing the outline of the contents alteration detection equipment of this operation gestalt. As shown in drawing 8 , the alteration detection system of this operation gestalt has server equipment 800, the EXIT gating arrangement 810, and client equipment 820.
[0052] Server equipment 800 is equipment which sticks IM which embedded the alteration detection information corresponding to registration of contents, or the contents at the time of updating, generates contents, and transmits the contents concerned to client equipment 820 through the EXIT gating arrangement 810.
[0053] The EXIT gating arrangement 810 is equipment which detects the alteration of the contents demanded from client equipment 820. Client equipment 820 is equipment which displays the contents to which the alteration of the contents received from the EXIT gating arrangement 810 is detected, and an alteration is not performed.
[0054] As shown in drawing 8 , with this operation gestalt, the EXIT gating arrangement 810 is formed between server equipment 800 and client equipment 820, and the EXIT gating arrangement 810 performs alteration detection using the check and IM of existence of IM. Moreover, by using together the check in client equipment 820, it is confirmed whether the alteration is performed on server equipment 800, the path from server equipment 800 to the EXIT gating arrangement 810, or the path from the EXIT gating arrangement 810 to client equipment 820.
[0055] Drawing 9 is drawing showing the outline configuration of the server equipment 800 of this operation gestalt. As shown in drawing 9 , the server equipment 800 of this operation gestalt has CPU901, memory 902, a magnetic disk drive 903, an input device 904, an output unit 905, CD-ROM equipment 906, the contents data 907, IM908, and creation information 909.
[0056] CPU901 is equipment which controls actuation of the server equipment 800 whole. In case memory 902 controls actuation of the server equipment 800 whole, it is storage which loads the various processing programs and data for it. A magnetic disk drive 903 is storage which stores said various processing programs and data.
[0057] An input unit 904 is equipment which performs the various inputs for registering contents or updating. An output unit 905 is equipment which performs the various outputs accompanying the registration and updating of contents. CD-ROM equipment 906 is equipment which reads the contents of the CD-ROM which recorded said various processing programs.
[0058] The contents data 907 are data in which the contents of the page exhibited according to the demand from client equipment 120 are shown. IM908 is the image data which embedded the alteration detection information corresponding to the contents data 907. Creation information 909 is data in which

the contents by which the alteration detection information for detecting the alteration of contents was generated are shown.
[0059] Moreover, server equipment 800 has IM generation processing section 910, the alteration detection information generation processing section 911, the creation information creation processing section 912, and the notice reception section 913 of an alteration.
[0060] IM generation processing section 910 is the processing section which generates IM908 which embedded the alteration detection information corresponding to the contents of contents. The alteration detection information generation processing section 911 is the processing section which generates the alteration detection information corresponding to the contents of contents.
[0061] The creation information creation processing section 912 is the processing section which creates the creation information 909 which shows the contents by which the alteration detection information for detecting the alteration of contents was generated. The notice reception section 913 of an alteration is the processing section which receives the notice which shows that the alteration of contents is performed from the EXIT gating arrangement 810.
[0062] After being recorded on record media, such as CD-ROM, and being stored in a magnetic disk etc., the program for operating server equipment 800 as IM generation processing section 910, the alteration detection information generation processing section 911, the creation information creation processing section 912, and the notice reception section 913 of an alteration shall be loaded to memory, and shall be performed. In addition, other record media other than CD-ROM are sufficient as the record medium which records said program.
[0063] Drawing 10 is drawing showing the outline configuration of the EXIT gating arrangement 810 of this operation gestalt. As shown in drawing 10 , the EXIT gating arrangement 810 of this operation gestalt has CPU1001, memory 1002, a magnetic disk drive 1003, an input unit 1004, an output unit 1005, and CD-ROM equipment 1006.
[0064] CPU1001 is equipment which controls actuation of the EXIT gating arrangement 810 whole. In case memory 1002 controls actuation of the EXIT gating arrangement 810 whole, it is storage which loads the various processing programs and data for it.
[0065] A magnetic disk drive 1003 is storage which stores said various processing programs and data. An input unit 1004 is equipment which performs the various inputs for detecting the alteration of contents. An output unit 1005 is equipment which performs the various outputs accompanying detection of an alteration of contents. CD-ROM equipment 1006 is equipment which reads the contents of the CD-ROM which recorded said various processing programs.
[0066] Moreover, the EXIT gating arrangement 810 has the generation-and-test processing section 1010, the existence inspection processing section 1011, the alteration detection information generation processing section 1012, and the alteration detection processing section 1013.
[0067] The generation-and-test processing section 1010 is the processing section which inspects whether the alteration detection information for detecting the alteration is generation ending about the contents demanded from client equipment 820 with reference to the creation information 909 which shows the contents by which the alteration detection information for detecting the alteration of contents was generated.
[0068] The existence inspection processing section 1011 is the processing section which inspects the existence of the alteration detection information on the contents about the contents demanded from client equipment 820. The alteration detection information generation processing section 1012 is the processing section which generates the alteration detection information corresponding to the current contents of contents demanded from client equipment 820.
[0069] When the alteration detection information corresponding to the contents and said generated alteration detection information at the time of registration of the contents concerned or updating are compared and the alteration of the contents concerned is detected, the alteration detection processing section 1013 It is the processing section which notifies having detected the alteration of the contents concerned on server equipment 800 or the path from server equipment 800 to the EXIT gating arrangement 810 to the server equipment 800 which is client equipment [which is the demand origin of the contents concerned] 820, and registration origin, and an updating agency.
[0070] After being recorded on record media, such as CD-ROM, and being stored in a magnetic disk etc., the program for operating the EXIT gating arrangement 810 as the generation-and-test processing section 1010, the existence inspection processing section 1011, the alteration detection information generation processing section 1012, and the alteration detection processing section 1013 shall be loaded

to memory, and shall be performed. In addition, other record media other than CD-ROM are sufficient as the record medium which records said program.

[0071] Drawing 11 is drawing showing the outline configuration of the client equipment 820 of this operation gestalt. As shown in drawing 11 , the client equipment 820 of this operation gestalt has CPU1101, memory 1102, a magnetic disk drive 1103, an input unit 1104, an output unit 1105, and CD-ROM equipment 1106.

[0072] CPU1101 is equipment which controls actuation of the client equipment 820 whole. In case memory 1102 controls actuation of the client equipment 820 whole, it is storage which loads the various processing programs and data for it.

[0073] A magnetic disk drive 1103 is storage which stores said various processing programs and data. An input unit 1104 is equipment which performs the various inputs for requiring and displaying contents. An output unit 1105 is equipment which displays contents with the demand of contents. CD-ROM equipment 1106 is equipment which reads the contents of the CD-ROM which recorded said various processing programs.

[0074] Moreover, client equipment 820 has the alteration detection information generation processing section 1110 and the alteration detection processing section 1111.

[0075] The alteration detection information generation processing section 1110 is the processing section which generates the alteration detection information corresponding to the current contents of reception and its contents for the demanded contents from the EXIT gating arrangement 810. The alteration detection processing section 1111 is the processing section which performs the display which shows that the alteration of the contents concerned on the path from the EXIT gating arrangement 810 to client equipment 820 was detected, when the alteration detection information corresponding to the contents and said generated alteration detection information at the time of registration of the contents concerned or updating are compared and the alteration of the contents concerned is detected.

[0076] After being recorded on record media, such as CD-ROM, and being stored in a magnetic disk etc., the program for operating client equipment 820 as the alteration detection information generation processing section 1110 and the alteration detection processing section 1111 shall be loaded to memory, and shall be performed. In addition, other record media other than CD-ROM are sufficient as the record medium which records said program.

[0077] Drawing 12 is a flow chart which shows the procedure of contents registration / update process of this operation gestalt. As shown in drawing 12 , after generating IM908 which embedded the alteration detection information corresponding to the contents of the contents to which registration and updating were performed with server equipment 800 and sticking on the contents concerned, processing which creates the creation information 909 which shows the contents to which attachment of IM908 was performed is performed.

[0078] When IM generation processing section 910 investigates whether the registration and updating of the contents data 907 were performed and the registration and updating of the contents data 907 are performed at step 1201, it progresses to step 1202.

[0079] At step 1202, about the contents to which registration and updating were performed, the hash value of the contents data 907 is calculated by the alteration detection information generation processing section 911, and it embeds as alteration detection information corresponding to the contents at IM908. And at step 1203, IM908 which embedded alteration detection information at step 1202 is stuck on the contents to which said registration and updating were performed.

[0080] The information the creation information creation processing section 912 indicates the contents to which attachment of IM908 was performed at step 1203 to be at step 1204 is set as creation information 909, and said set-up creation information 909 is sent to the EXIT gating arrangement 810 at step 1205.

[0081] Drawing 13 is drawing showing an example of the creation information 909 of this operation gestalt. As shown in drawing 13 , information, such as generation date time of day of the file name containing the pathname of the contents data 907 with which attachment of IM908 was performed, or stuck IM908, is set to creation information 909 as information which shows the contents to which attachment of IM908 was performed.

[0082] Drawing 14 is a flow chart which shows the procedure of client side processing of this operation gestalt. As shown in drawing 14 , client equipment 820 performs processing which generates the alteration detection information corresponding to the present contents of reception and its contents for the demanded contents from the EXIT gating arrangement 810, and detects an alteration.

[0083] At step 1401, when it investigates whether the user inputted URL (Uniform Resource Locators) and a user inputs URL, the WWW browser of client equipment 820 receives the URL, and progresses to step 1402. At step 1402, the request for displaying the page of the reception beam URL at step 1401 is transmitted to the destination shown by said URL. The destination shown by said URL is server equipment 800, and when the EXIT gating arrangement 810 is on the path, said request is sent to server equipment 800 via the EXIT gating arrangement 810.
[0084] At step 1403, it investigates whether HTML data are received as a result of said transmitted request, and when HTML data are received, it progresses to step 1404.
[0085] At step 1404, when it investigates whether IM908 is stuck and IM908 is stuck into the HTML data received at step 1403, it progresses to step 1405, and when IM908 is not stuck, it progresses to step 1406.
[0086] The alteration detection processing section 1111 investigates whether about the HTML data received at step 1403, the hash value to the contents is calculated by the alteration detection information generation processing section 1110, the hash value and said calculated hash value in IM908 are compared, and the alteration of the contents concerned is performed at step 1405. As a result of investigating whether the alteration of the contents concerned is performed, when the alteration of the contents concerned is not detected, it progresses to step 1406, and when the alteration of the contents concerned is detected, it progresses to step 1407.
[0087] According to the HTML data received at step 1403, a page is expressed as step 1406. Since the HTML data in which it is shown that the alteration was detected have been sent from the EXIT gating arrangement 810 when processing the request of said URL here and the EXIT gating arrangement 810 detects the alteration which is the page concerned, with client equipment 820, the display which shows that the alteration of the page concerned was detected with the EXIT gating arrangement 810 is performed.
[0088] It investigates whether the information which shows that processing with the EXIT gating arrangement 810 was performed into the HTML data received at step 1403 is included, at step 1407, when the information which shows that processing with the EXIT gating arrangement 810 was performed is included, it progresses to step 1408, and when not contained, it progresses to step 1409.
[0089] At step 1408, the display which shows that the alteration of the contents concerned on the path from the EXIT gating arrangement 810 to client equipment 820 was detected is performed, and the display which shows that the alteration of the contents concerned was only detected is performed in step 1409.
[0090] Drawing 15 is a flow chart which shows the procedure of EXIT gate side processing of this operation gestalt. When it investigates whether the alteration detection processing section 1013 of the EXIT gating arrangement 810 has received the request from client equipment 820 and the request is received at step 1501, it progresses to step 1502.
[0091] In step 1502, it investigates whether the contents data 907 demanded at the request concerned are held as a cache, and when not holding, the request concerned is sent to server equipment 800 at step 1503.
[0092] At step 1504, it investigates whether the HTML data corresponding to the request concerned are received from server equipment 800, and when HTML data are received, it progresses to step 1505.
[0093] Refer to the creation information 909 which shows the contents by which the alteration detection information for detecting the alteration of contents was generated for the generation-and-test processing section 1010 at step 1505. At step 1506, it investigates whether the alteration detection information for detecting the alteration is generation ending about the contents demanded from client equipment 820, and when alteration detection information is generation ending, it progresses to step 1507.
[0094] At step 1507, the existence inspection processing section 1011 investigates whether IM908 shown by creation information 909 is stuck into the HTML data received at step 1504, and performs processing which inspects the existence of the alteration detection information on the contents about the contents demanded from client equipment 820. When IM908 shown by creation information 909 is stuck, it progresses to step 1508, and when IM908 shown by creation information 909 is not stuck, it progresses to step 1511.
[0095] The alteration detection processing section 1013 investigates whether about the HTML data received at step 1504, the hash value to the contents is calculated by the alteration detection information generation processing section 1012, the hash value and said calculated hash value in IM908 are compared, and the alteration of the contents concerned is performed at step 1508. As a result of

investigating whether the alteration of the contents concerned is performed, when the alteration of the contents concerned is not detected, it progresses to step 1509, and when the alteration of the contents concerned is detected, it progresses to step 1512.
[0096] At step 1509, the contents data 907 which are HTML data received at step 1504 are held as a cache, and the HTML data concerned are transmitted to client equipment 820 in step 1510 with the information which shows that processing with the EXIT gating arrangement 810 was performed.
[0097] At step 1511, the display which shows that removal of the alteration detection information on the contents concerned on server equipment 800 or the path from server equipment 800 to the EXIT gating arrangement 810 was detected is performed. Moreover, at step 1512, the display which shows that the alteration of the contents of the contents concerned on server equipment 800 or the path from server equipment 800 to the EXIT gating arrangement 810 was detected is performed.
[0098] At step 1513, processing which notifies that removal of the alteration detection information on the contents concerned or the alteration of the contents of the contents concerned was performed to the server equipment 800 which is the registration origin of the contents concerned and an updating agency on server equipment 800 or the path from server equipment 800 to the EXIT gating arrangement 810 is performed.
[0099] Moreover, at step 1513, processing which notifies that removal of the alteration detection information on the contents concerned or the alteration of the contents of the contents concerned was performed to the client equipment 820 which is the demand origin of the contents concerned on server equipment 800 or the path from server equipment 800 to the EXIT gating arrangement 810 is performed.

[0100] Drawing 16 is a flow chart which shows the procedure of the notice reception section 913 of an alteration of this operation gestalt. As shown in drawing 16 , the notice reception section 913 of an alteration of server equipment 800 performs processing which receives the notice which shows that the alteration of contents is performed from the EXIT gating arrangement 810.
[0101] At step 1601, the notice reception section 913 of an alteration investigates whether the notice which shows that the alteration of contents is performed is received from the EXIT gating arrangement 810, and when the notice which shows that the alteration of contents is performed is received, it progresses to step 1602. At step 1602, the received contents of a notice are displayed, the manager of server equipment 800 is told, and the received contents of a notice are stored in a magnetic disk drive 903 in step 1603.
[0102] It is possible to prevent concealment of the alteration by removal of alteration detection information since the existence of alteration detection information is inspected like according to the contents alteration detection equipment of this operation gestalt when it explained above.
[0103] Moreover, according to the contents alteration detection equipment of this operation gestalt, since the alteration of contents is detected between a client and a server, it is possible to pinpoint the location in.
[0104]
[Effect of the Invention] Since the configuration of two or more contents or the alteration of the contents is detected according to this invention, it is possible to carry out early detection of the alteration of contents.

[Translation done.]

* NOTICES *

1.This document has been translated by computer. So the translation may not reflect the original precisely.
2.**** shows the word which can not be translated.
3.In the drawings, any words are not translated.

DRAWINGS

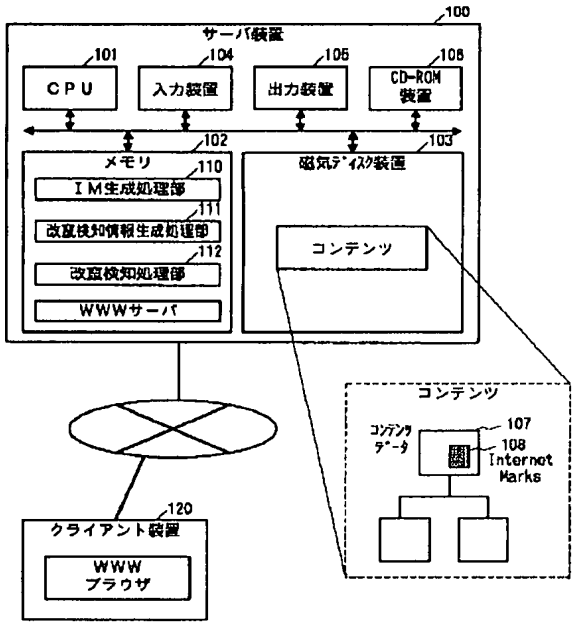
[Drawing 13]

図１３

ファイル名	日付時刻	…
index.html	2000/3/26 11:06	…
down¥content2.html	2000/3/26 11:16	…
:	:	…

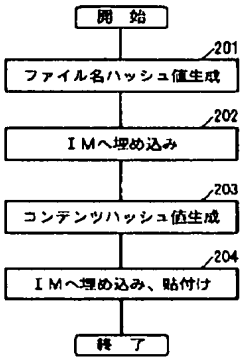
[Drawing 1]

図１



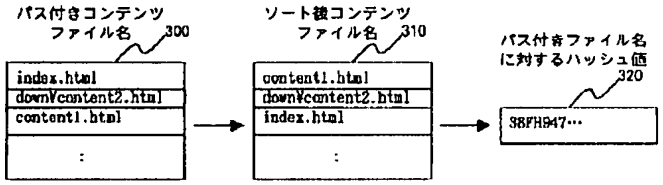
[Drawing 2]

図２



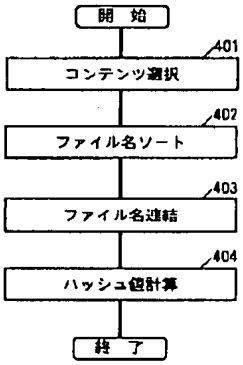
[Drawing 3]

図3



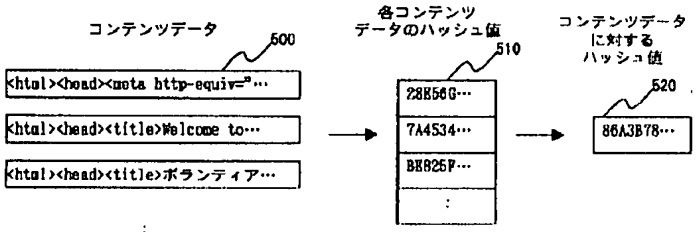
[Drawing 4]

図4



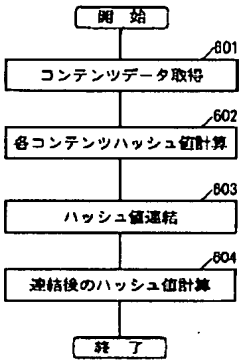
[Drawing 5]

図5



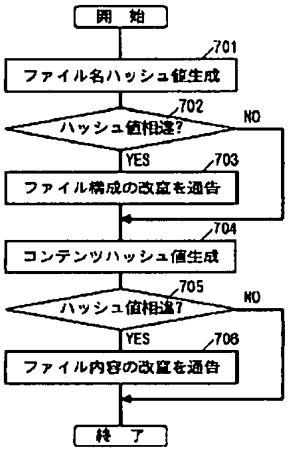
[Drawing 6]

図6



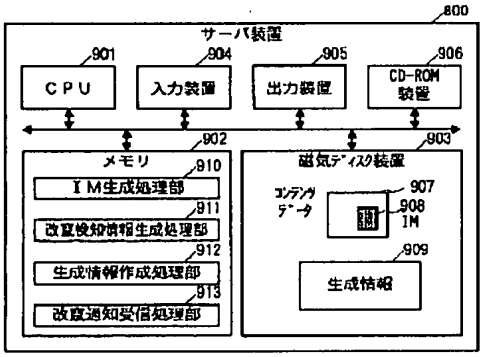
[Drawing 7]

図 7



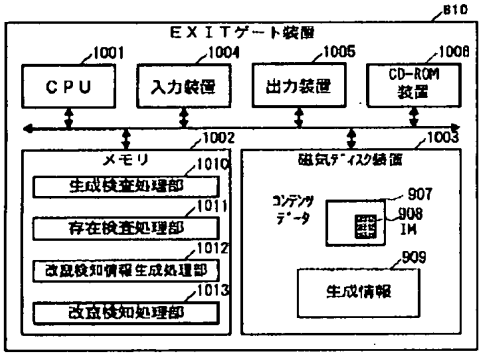
[Drawing 9]

図 9



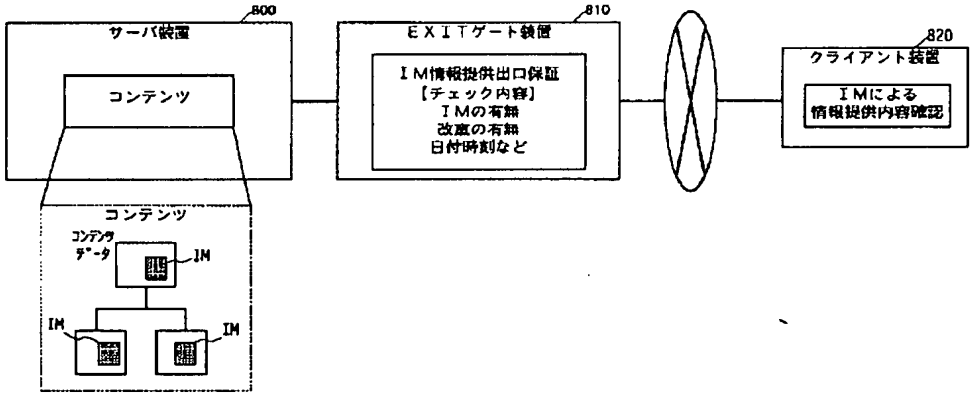
[Drawing 10]

図 1 0



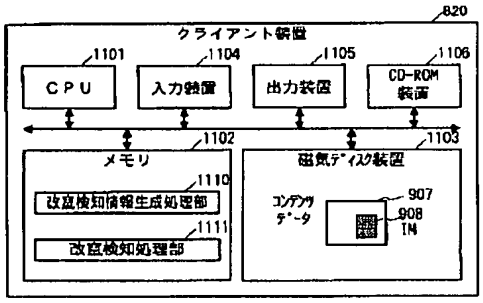
[Drawing 8]

図８



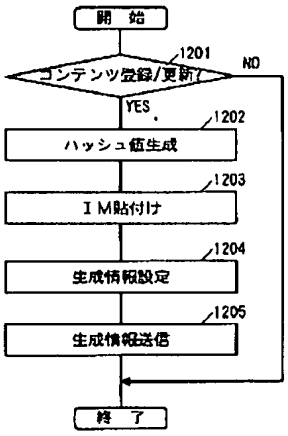
[Drawing 11]

図１１



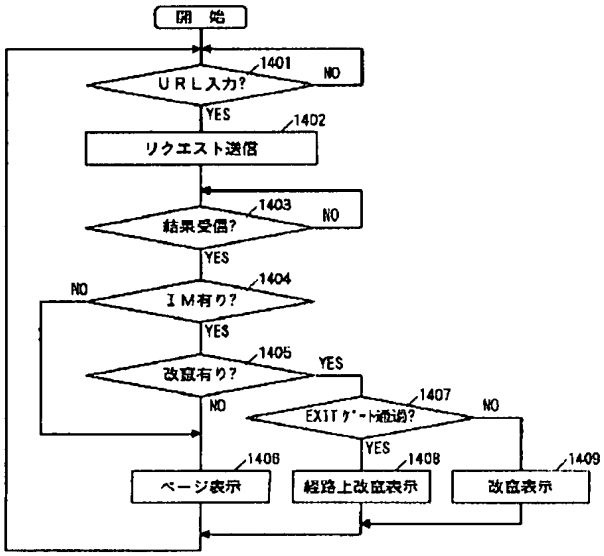
[Drawing 12]

図１２



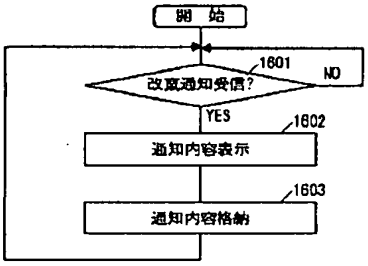
[Drawing 14]

図１４



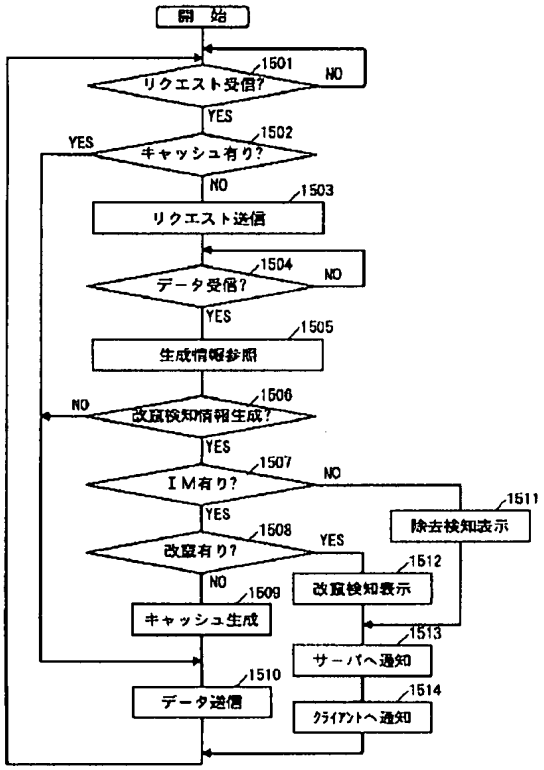
[Drawing 16]

図１６



[Drawing 15]

図１５



[Translation done.]